#4

מדינת ישראל
STATE OF ISRAEL

CERTIFIED COPY OF PRIORITY DOCUMENT

Ministry of Justice
Patent Office

משרד המשפטים
לשכת הפטנטים

This is to certify that annexed hereto is a true copy of the documents as originally deposited with the patent application of which particulars are specified on the first page of the annex.

זאת לתעודה כי רצופים בזה העתקים נכונים של המסמכים שהופקדו לכתחילה עם הבקשה לפטנט לפי הפרטים הרשומים בעמוד הראשון של הנספח.

This 26-06-2001 היום

ש. לשרי
ממונה על הבוחנים
רשם הפטנטים
Commissioner of Patents

CERTIFIED COPY OF PRIORITY DOCUMENT

נתאשר
Certified

חוק הפטנטים, תשכ"ז-1967
Patent Law, 5727 - 1967

בקשה לפטנט
Application for Patent

לשימוש הלישכה
For Office Use

מספר: Number	135246
תאריך: Date	23-03-2000
הוקדם/נדחה Ante/Post-Dated	

אני, (שם המבקש, מענו ולגבי גוף מאוגד - מקום התאגדותו)
I, (Name and address of applicant, and in case of body corporate-place of incorporation)

CIPHERIT LTD.

סייפריט בע"מ
רח' סיגלון 38
עומר 84965

Inventor: הממציא:
בנימין ארזי
Benjamin ARAZI

בעל ההמצאה מכח הדין THE LAW ששמה הוא
Owner, by virtue of an invention the title of which is

(בעברית) (Hebrew)
שיטות ומערכות לאישור שרשרת יעיל

(באנגלית) (English)
METHODS AND SYSTEMS FOR EFFICIENT CHAINED CERTIFICATION

hereby apply for a patent to be granted to me in respect thereof. מבקש בזאת כי ינתן לי עליה פטנט

*בקשת חלוקה - Application of Division	*בקשת פטנט מוסף - Application for Patent Addition	*דרישה דין קדימה Priority Claim		
*מבקשת פטנט from Application	*לבקשה/לפטנט to Patent/Appl.	מספר/סימן Number/Mark	תאריך Date	מדינת האיגוד Convention Country
№ ____ מס'	№ ____ מס'			
dated ____ מיום	dated ____ מיום			

*יפוי כח: כללי / ~~מיוחד - רצוף בזה / עוד יוגש~~
P.O.A.: general / ~~individual - attached / to be filed later~~
filed in case 121297 הוגש בענין

המען למסירת מסמכים בישראל
Address for Service in Israel
לוצאטו את לוצאטו
ת.ד. 5352
באר שבע 84152
מספרנו: 11002/00

היום 22 בחודש מרץ שנה 2000
This 22 of February of the year 2000

חתימת המבקש
Signature of Applicant

Luzzatto & Luzzatto
By:
Attorneys for Applicant

לשימוש הלישכה

טופס זה כשהוא מוטבע בחותם לישכת הפטנטים ומושלם במספר ובתאריך ההגשה, הינו אישור להגשת הבקשה שפרטיה רשומים לעיל.
This form, impressed with the Seal of the Patent Office and indicating the number and date of filing, certifies the filing of the application the particulars of which are set out above.

* מחק את המיותר Delete whatever is inapplicable

METHODS AND SYSTEMS FOR EFFICIENT CHAINED CERTIFICATION

Field of The Invention

The present invention relates to systems and methods for efficiently chaining a certification in a PKI (Public Key Infrastructure), from a Certifying Authority to end users, using operations over elliptic curves and modular exponentiations over finite fields or groups.

Background of the Invention

The validity of public key cryptographic applications is based on the assumption that the public key $\mathbf{Y}_i$ submitted by a user, termed $User_i$, is valid. That is, $\mathbf{Y}_i$ is assumed to be undeniably associated with the identification details, termed ID_i, of $User_i$. Verifying the validity of $\mathbf{Y}_i$ is commonly done, by the recipient, by referring to a certificate, which is submitted by $User_i$ together with $\mathbf{Y}_i$ and ID_i.

Said certificate consists of the signature of a CA (Certifying Authority) on the association between $\mathbf{Y}_i$ and ID_i. In order to generate said certificate, said CA uses his private key, according to the concept of public key cryptography.

Upon receiving $\mathbf{Y}_i$ and ID_i and said certificate, the recipient verifies the correct association between $\mathbf{Y}_i$ and ID_i by referring to said certificate and effecting a signature verification procedure, using the public key of said CA.

When using digital signature procedures based on the discrete logarithm problem, said signature verification procedure is based on effecting two modular exponentiation operations as clear to persons skilled in the art.

In a 'chained certification', a $User_i$ attests the association between the public key and the identification details of another user, termed $User_{(i+1)}$. $User_{(i+1)}$ attests the association between the public key and the identification details of $User_{(i+2)}$, etc. (The

index i refers to the hierarchical level, in a certification chain, of a user, with respect to the CA, who acts as $User_0$.)

Using customary certification approaches, said $User_i$, starting with the CA who acts as $User_0$, signs the association between the public key and the identification details of said $User_{(i+1)}$ by generating an explicit signature, generating the certificate $Cert_{(i+1)}$. Using signature methods which are based on the discrete logarithm problem, a certificate $Cert_i$ is a pair $\{c_i,\mathbf{B}_i\}$, where c_i is a scalar and $\mathbf{B}_i$ is a group-element over which the discrete logarithm problem applies.

To verify the correct association between said public key of said $User_{(i+1)}$ and said identification details of said $User_{(i+1)}$, a verifier needs to know the public keys and the identification details of all users from $User_1$ to $User_{(i+1)}$. The verifier further needs to know the public key of the CA (as was said, the CA acts as $User_0$) and all certificates from $Cert_1$ to $Cert_{(i+1)}$. Based on said values, the verifier effects i+1 signature verification procedures, where each such signature verification requires two modular exponentiations. Altogether, said verifier performs 2(i+1) exponentiation operations.

The art has so far failed to provide means by which chained certificate verification can be effectively implemented by saving mathematical operations, permitting to use less computational operations in effecting certification verification.

It is therefore an object of the present invention to provide a method by which chained certificate verification can be carried out with high efficiency.

Other objects of the invention will become apparent as the description proceeds.

SUMMARY OF THE INVENTION

The invention relates to a method for effecting a chained key-issuing process over a finite group of points in which the discrete logarithm problem applies, wherein an issuing user ($User_i$), who possesses an issuing user public value ($\mathbf{U}_i$) and an issuing user private key (x_i), provides to a successor user ($User_{(i+1)}$) a successor user public value ($\mathbf{U}_{(i+1)}$) and a successor user private key ($x_{(i+1)}$), and where said issuing user, except for the Certifying Authority (CA), was himself a successor user in a preceding step in the chained key-issuing process, and where said Certifying Authority acts as the first issuing user in the chained key-issuing process, comprising the steps of:

(1) permitting said Certifying Authority to select a generating group-point (**G**) whose exponentiations to various powers generate various group-points and a converting mathematical operation (H) which converts several input values into a scalar;

(2) permitting said Certifying Authority to posses a Certifying Authority private key (x_0);

(3) permitting said Certifying Authority to posses a Certifying Authority public value ($\mathbf{U}_0$), obtained by exponentiating said generating group-point to the power of said Certifying Authority private key ($\mathbf{U}_0 = x_0 * \mathbf{G}$);

(4) permitting said issuing user ($User_i$) to possess said generating group-point (**G**) and said converting mathematical operation (H) and the identification details ($ID_{(i+1)}$) of said successor user;

(5) permitting said issuing user ($User_i$) to possess an issuing user private key (x_i), where, except for the case in which said issuing user is said Certifying Authority, said issuing user private key was provided to said issuing user at a preceding stage in the chained key-issuing process (in which $User_i$ acted as a successor user in respect to an issuing $User_{(i-1)}$);

(6) permitting said issuing user ($User_i$) to calculate said successor user public value ($\mathbf{U}_{(i+1)}$) and said successor user private key ($x_{(i+1)}$) wherein:

- a successor user random value ($k_{(i+1)}$) is generated and said successor user public value ($\mathbf{U}_{(i+1)}$) is calculated by exponentiating said generating group-point to the power of said successor user random value ($\mathbf{U}_{(i+1)} = k_{(i+1)} * \mathbf{G}$);

- a successor user representing value ($H(ID_{(i+1)},\mathbf{U}_{(i+1)})$) is calculated by operating with said converting mathematical operation on said successor user identification details ($ID_{(i+1)}$) and said successor user public value ($\mathbf{U}_{(i+1)}$);

- said successor user private key ($x_{(i+1)}$) is calculated by multiplying said successor user representing value ($H(ID_{(i+1)},\mathbf{U}_{(i+1)})$) by said successor user random value ($k_{(i+1)}$) and adding said issuing user private key (x_i) to the product obtained by said multiplication ($x_{(i+1)} = H(ID_{(i+1)},\mathbf{U}_{(i+1)}) * k_{(i+1)} + x_i$) and reducing the result modulo the order of said generating group-point;

(7) permitting said issuing user ($User_i$) to submit said successor user public value ($\mathbf{U}_{(i+1)}$) and said successor user private key ($x_{(i+1)}$) to said successor user ($User_{(i+1)}$).

According to a preferred embodiment of the invention there is provided a method where the issuing user ($User_i$) does not know the successor user private key ($x_{(i+1)}$), further comprising the steps of:

(i) permitting said successor user ($User_{(i+1)}$) to generate a first random value ($m_{(i+1)}$) and calculate a first intermediate group-point ($m_{(i+1)} * \mathbf{G}$) by exponentiating the generating group-point to the power of said first random value;

(ii) permitting said successor user to submit said first intermediate group-point ($m_{(i+1)} * \mathbf{G}$) to said issuing user ($User_i$);

(iii) permitting said issuing user to calculate a successor user public value ($\mathbf{U}_{(i+1)}$) and a successor user intermediate private key ($p_{(i+1)}$), wherein:

- a second random value ($k_{(i+1)}$) is generated and a second intermediate group-point ($k_{(i+1)}*\mathbf{G}$) is calculated by exponentiating said generating group-point to the power of said second random value;

- said successor user public value ($\mathbf{U}_{(i+1)}$) is calculated by adding said first intermediate group-point and said second intermediate group-point ($\mathbf{U}_{(i+1)}= m_{(i+1)}*\mathbf{G} + k_{(i+1)}*\mathbf{G}$);

- a successor user representing value ($H(ID_{(i+1)},\mathbf{U}_{(i+1)})$) is calculated in the way described;

- said successor user intermediate private key ($p_{(i+1)}$) is calculated by multiplying said successor user representing value ($H(ID_{(i+1)},\mathbf{U}_{(i+1)})$) by said second random value ($k_{(i+1)}$) and adding the issuing user private key (x_i) to the product obtained by said multiplication ($p_{(i+1)} = H(ID_{(i+1)},\mathbf{U}_{(i+1)})*k_{(i+1)} + x_i$) and reducing the result modulo the order of said generating group-point;

(iv) permitting said successor user to generate the successor user private key ($x_{(i+1)}$) by calculating said successor user representing value ($H(ID_{(i+1)},\mathbf{U}_{(i+1)})$) in the way described and multiplying said successor user representing value by said first random value ($m_{(i+1)}$) and adding said successor user intermediate private key ($p_{(i+1)}$) to the product obtained by said multiplication ($x_{(i+1)} = H(ID_{(i+1)},\mathbf{U}_{(i+1)})*m_{(i+1)} + p_{(i+1)}$) and reducing the result modulo the order of said generating group-point.

In another aspect the invention is directed to a certificate generation system for permitting a generating user who is a successor user ($User_{(i+1)}$) according to the aforementioned method of the invention, to issue a certificate to a general user ($User_{(i+2)}$) where said certificate attests to the association between said general user public key ($\mathbf{Y}_{(i+2)}$) and said general user identification details ($ID_{(i+2)}$), where said general user public key was issued to said general user according to any known public key cryptographic method, the system comprising:

(1) means for permitting said generating user to generate a first random scalar ($k_{(i+2)}$);

(2) means for permitting said generating user to calculate a first part of a certificate ($\mathbf{T}_{(i+2)}$) by exponentiating the generating group-point to the power of said first random scalar ($\mathbf{T}_{(i+2)} = k_{(i+2)} * \mathbf{G}$);

(3) means for permitting said generating user to calculate a general user representing value ($H(ID_{(i+2)},\mathbf{Y}_{(i+2)},\mathbf{T}_{(i+2)})$) by operating with the converting mathematical operation on said general user identification details ($ID_{(i+2)}$) and said general user public key ($\mathbf{Y}_{(i+2)}$) and said first part of a certificate ($\mathbf{T}_{(i+2)}$);

(4) means for permitting said generating user to calculate a second part of a certificate ($s_{(i+2)}$) by multiplying said general user representing value by said first random scalar ($k_{(i+2)}$) and adding the private key ($x_{(i+1)}$) of said generating user to the product obtained by said multiplication ($s_{(i+2)} = H(ID_{(i+2)},\mathbf{Y}_{(i+2)},\mathbf{T}_{(i+2)}) * k_{(i+2)} + x_{(i+1)}$) and reducing the result modulo the order of said generating group-point;

(5) means for permitting said generating user to submit said certificate to said general user, said certificate comprising of said first part of a certificate ($\mathbf{T}_{(i+2)}$) and said second part of a certificate ($s_{(i+2)}$).

According to a preferred embodiment of the invention there is provided a chained certificate verification system for permitting a verifying user to verify the authenticity of the certificate ($\mathbf{T}_{(i+2)}$ and $s_{(i+2)}$) issued to the general user ($User_{(i+2)}$), as defined above, the system comprising:

(1) means for providing said verifying user with said certificate and with the general user public key ($\mathbf{Y}_{(i+2)}$) and with the general user identification details ($ID_{(i+2)}$) and with the Certifying Authority public value ($\mathbf{U}_0$) and with a plurality of pairs of values (ID_j and $\mathbf{U}_j$) consisting of the identification details and public values of all users ($User_j$, $j = 1, 2, \ldots, i+1$)) in the chained

key-issuing process as defined in Claim 1, starting with the first successor user ($User_1$) after the Certifying Authority and ending with the generating user ($User_{(i+1)}$) as hereinbefore defined;

(2) means for permitting said verifying user to verify the validity of said certificate, wherein:

- a first scalar ($H(ID_{(i+2)},\mathbf{Y}_{(i+2)},\mathbf{T}_{(i+2)})$) is calculated by operating with the converting mathematical operation on said general user identification details ($ID_{(i+2)}$) and said general user public key ($\mathbf{Y}_{(i+2)}$) and the first part of said certificate ($\mathbf{T}_{(i+2)}$);

- a first intermediate group-point ($H(ID_{(i+2)},\mathbf{Y}_{(i+2)},\mathbf{T}_{(i+2)})*\mathbf{T}_{(i+2)}$) is calculated by exponentiating said first part of the certificate ($\mathbf{T}_{(i+2)}$) to the power of said first scalar;

- users representing values ($H(ID_j,\mathbf{U}_j)$, $j = 1, 2,\ldots, i+1$) are calculated by operating with said converting mathematical operation on each pair of said plurality of pairs of values (ID_j and $\mathbf{U}_j$);

- users temporary group-points ($H(ID_j,\mathbf{U}_j)*\mathbf{U}_j$, $j = 1, 2,\ldots, i+1$) are calculated for each user in said chained key-issuing process, starting with said first successor user ($User_1$) and ending with said generating user ($User_{(i+1)}$), by exponentiating each said user public value ($\mathbf{U}_j$) to the power of said user representing value ($H(ID_j,\mathbf{U}_j)$);

- a second intermediate group-point ($\mathbf{P}$) is calculated by adding all said users temporary group-points ($\mathbf{P} = H(ID_{(i+1)},\mathbf{U}_{(i+1)})*\mathbf{U}_{(i+1)} + H(ID_i,\mathbf{U}_i)*\mathbf{U}_i + H(ID_{(i-1)},\mathbf{U}_{(i-1)})*\mathbf{U}_{(i-1)} + \ldots + H(ID_1,\mathbf{U}_1)*\mathbf{U}_1$);

- a third intermediate group-point ($\mathbf{Q}$) is calculated by adding said first intermediate group-point and said second intermediate group-point and the public value of said Certifying Authority ($\mathbf{Q} = H(ID_{(i+2)},\mathbf{Y}_{(i+2)},\mathbf{T}_{(i+2)})*\mathbf{T}_{(i+2)} + \mathbf{P} + \mathbf{U}_0$);

- a fourth intermediate group-point ($s_{(i+2)}*\mathbf{G}$) is calculated by exponentiating the generating group-point to the power of the first part ($s_{(i+2)}$) of said certificate;

- the value of said fourth intermediate group-point ($s_{(i+2)}*\mathbf{G}$) is compared to that of said third intermediate group-point (**Q**) and the certificate is determined as being valid in the case of equality.

In a further aspect the invention encompasses a chained signature generation and verification system for permitting a successor user ($User_{(i+1)}$) according to the method of the invention, to generate a signature and permitting a verifying party to verify said signature, the system comprising:

(1) means for permitting said successor user ($User_{(i+1)}$) to generate a signature on a message (m) wherein:

- a first scalar (k) is randomly generated;

- a first part of a signature (**T**) is generated by exponentiating the generating group-point to the power of said first scalar ($\mathbf{T} = k*\mathbf{G}$);

- a representing value ($H(m,\mathbf{T})$) is generated by operating with the converting mathematical operation on said message (m) and said first part of a signature (**T**);

- a second part of a signature (s) is calculated by multiplying said representing value ($H(m,\mathbf{T})$) by said first scalar (k) and adding the private key of said successor user ($x_{(i+1)}$) to the product obtained by said multiplication ($s = H(m,\mathbf{T})*k + x_{(i+1)}$) and reducing the result modulo the order of said generating group-point;

(2) means for permitting said successor user to submit said message (m) and said signature (**T** and s) to said verifying party, said signature comprising of said first part of a signature (**T**) and said second part of a signature (s);

(3) means for providing said verifying party with the Certifying Authority public value (**U_0**) and with a plurality of pairs of values (ID_j and **U_j**) consisting of the identification details and public values (ID_j and **U_j**) of all users ($User_j$, $j = 1, 2, \ldots, i+1$)) in the chained key-issuing process as hereinbefore defined, starting with the first successor user ($User_1$) after the Certifying Authority and ending with said successor user ($User_{(i+1)}$));

(4) means for permitting said verifying party to verify the validity of said signature (**T** and s) on said message (m), wherein:

- said representing value (H(m,**T**)) is generated in the way described;

- a first intermediate group-point ($H(m,\mathbf{T})*\mathbf{T}$) is calculated by exponentiating said first part of the signature (**T**) to the power of said representing value;

- users representing values ($H(ID_j,\mathbf{U_j})$, $j = 1, 2, \ldots, i+1$) are calculated by operating with said converting mathematical operation on each pair of said plurality of pairs of values (ID_j and **U_j**);

- users temporary group-points ($H(ID_j,\mathbf{U_j})*\mathbf{U_j}$, $j = 1, 2, \ldots, i+1$) are calculated for each user in said chained key-issuing process, starting with said first successor user ($User_1$) and ending with said successor user ($User_{(i+1)}$)), by exponentiating each said user public value (**U_j**) to the power of said user representing value ($H(ID_j,\mathbf{U_j})$);

- a second intermediate group-point (**P**) is calculated by adding all said temporary group-points ($\mathbf{P} = H(ID_{(i+1)},\mathbf{U_{(i+1)}})*\mathbf{U_{(i+1)}} + H(ID_i,\mathbf{U_i})*\mathbf{U_i} + H(ID_{(i-1)},\mathbf{U_{(i-1)}})*\mathbf{U_{(i-1)}} + \ldots + H(ID_1,\mathbf{U_1})*\mathbf{U_1}$);

- a third intermediate group-point (**Q**) is calculated by adding said first intermediate group-point and said second intermediate group-point and the public value of said Certifying Authority ($\mathbf{Q} = H(m,\mathbf{T})*\mathbf{T} + \mathbf{P} + \mathbf{U_0}$);

- a fourth intermediate group-point (s∗**G**) is calculated by exponentiating the generating group-point to the power of the first part (s) of said signature;

- the value of said fourth intermediate group-point (s∗**G**) is compared to that of said third intermediate group-point (**Q**) and the signature is determined as being valid in the case of equality.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

All the above and other characteristics and advantages of the invention, though clear to the skilled person, will be better understood through the following illustrative and non-limitative description of preferred embodiments thereof.

The implementations rely on a finite group of points over which the discrete logarithm problem applies.

The following notations and terms are used throughout the description of the various embodiments of this invention:

The term "group-point" refers to an element of a finite group of points in which the discrete logarithm problem applies.

A group-point is denoted in **bold**.

s∗**P** is a group-point obtained by exponentiating the group-point **P** to the power s.

A 'scalar' is a value which acts as an exponent. It is denoted by lower-case letters.

The '+' notation in the expression s∗**P** + t∗**Q** means an addition of two group-points under the specific features of said finite group of points.

G denotes a generating group-point, joint to all users of a given system.

Log**P** is the scalar k such that $\mathbf{P} = k*\mathbf{G}$. Note that $\log(\mathbf{A}+\mathbf{B}) = \mathrm{Log}\mathbf{A} + \mathrm{Log}\mathbf{B}$.

Scalars are calculated modulo the order of **G**.

CA - The Certifying Authority.

$User_i$ the i-th user in a certification chain (in which the CA is $User_0$).

x_i - the private key of $User_i$.

$\mathbf{U}_i$ - the public value of $User_i$. $User_i$, except for $User_0$ (which is the CA), does not know $\log\mathbf{U}_i$.

$H(c,\mathbf{B},\mathbf{D})$, $H(c,\mathbf{B})$, $H(\mathbf{B})$ – a mathematical operation, known to the CA and to all users, that converts a scalar and two group-points, or a scalar and a group-point, or a group-point, into a scalar. For the case of operating over elliptic-curves, a preferred implementation of the operation $H(\mathbf{B})$ is taking the value of the x-coordinate of the group-point **B**.

A preferred first embodiment of this invention concerns a chained key-issuing method wherein a user, termed $User_i$, provides personal keys to another user, termed $User_{(i+1)}$, and where the Certifying Authority, termed CA, acts as $User_0$. Said personal keys, which consist of a private key $x_{(i+1)}$ and a public value $\mathbf{U}_{(i+1)}$ and which are distinct for each user, are provided for the purpose of effecting public key cryptographic operations over a finite group of points in which the discrete logarithm problem applies.
The identification details of said $User_{(i+1)}$ are termed $ID_{(i+1)}$. The private key of said $User_i$ is a scalar x_i.
$User_i$ performs the following operations:

generate a random $k_{(i+1)}$;

calculate $\mathbf{U}_{(i+1)} = k_{(i+1)}*\mathbf{G}$, for a generating group-point **G**, joint to all users;

calculate $x_{(i+1)} = H(ID_{(i+1)},\mathbf{U}_{(i+1)})*k_{(i+1)} + x_i$

where $H(c,\mathbf{B})$ is a compressing mathematical operation, known to the CA and to all users, that converts the group-point **B** and a scalar c into a scalar.

$x_{(i+1)}$, like other scalars calculated in the processes included in this invention, is calculated modulo the order of said generating group-point $\mathbf{G}$, as will be clear to persons skilled in the art.

Said $User_i$ issues said values $x_{(i+1)}$ and $\mathbf{U}_{(i+1)}$ to said $User_{(i+1)}$. These two values serve, respectively, as the user's private value and the user's public value. In this case, the private key $x_{(i+1)}$ of $User_{(i+1)}$ is known to $User_i$.

Said $User_{(i+1)}$ is also provided with the public value $\mathbf{U_0}$ of the CA and the identification details ID_j and public values $\mathbf{U_j}$, for $j = 1, 2, \ldots, i$. (That is, said $User_{(i+1)}$ is provided with the identification details and public values of all users that preceded him in the certification chain.)

Said $User_{(i+1)}$ can establish the validity of said values $x_{(i+1)}$ and $\mathbf{U}_{(i+1)}$ issued to him by said $User_i$ by checking whether $x_{(i+1)}*\mathbf{G} = H(ID_{(i+1)},U_{(i+1)})*\mathbf{U}_{(i+1)} + H(ID_i,U_i)*\mathbf{U_i} + H(ID_{(i-1)},U_{(i-1)})*\mathbf{U}_{(i-1)} + \ldots + H(ID_1,U_1)*\mathbf{U_1} + \mathbf{U_0}$.

A preferred second embodiment of this invention concerns a method, which is an alternative to the method according to said preferred first embodiment of this invention, by which $User_i$ provides personal keys to $User_{(i+1)}$.

According to said preferred second embodiment of this invention, and using the same notations used in said preferred first embodiment of this invention, said $User_{(i+1)}$ generates a random $m_{(i+1)}$ and submits $m_{(i+1)}*\mathbf{G}$ to said $User_i$. Said $User_i$ performs the following operations:

generate a random $k_{(i+1)}$;

calculate $k_{(i+1)}*\mathbf{G}$ and $\mathbf{U}_{(i+1)} = m_{(i+1)}*\mathbf{G} + k_{(i+1)}*\mathbf{G}$;

calculate $p_{(i+1)} = H(ID_{(i+1)},\mathbf{U}_{(i+1)})*k_{(i+1)} + x_i$

Said $User_i$ issues said values $p_{(i+1)}$ and $\mathbf{U}_{(i+1)}$ to said $User_{(i+1)}$.

Said $User_{(i+1)}$ generates his private key $x_{(i+1)} = p_{(i+1)} + H(ID_{(i+1)},U_{(i+1)})*m_{(i+1)}$.

That is: $x_{(i+1)} = H(ID_{(i+1)},\mathbf{U}_{(i+1)})*(k_{(i+1)}+m_{(i+1)}) + x_i$.

Said $User_{(i+1)}$ can establish the validity of the values $p_{(i+1)}$ and $\mathbf{U}_{(i+1)}$ issued to him by said $User_i$ checking whether

$p_{(i+1)}*\mathbf{G} = H(ID_{(i+1)},\mathbf{U}_{(i+1)})*(k_{(i+1)}*\mathbf{G}) + H(ID_i,\mathbf{U}_i)*\mathbf{U}_i + H(ID_{(i-1)},\mathbf{U}_{(i-1)})*\mathbf{U}_{(i-1)} + \ldots + H(ID_1,\mathbf{U}_1)*\mathbf{U}_1 + \mathbf{U}_0$.

($User_{(i+1)}$ calculates $k_{(i+1)}*\mathbf{G}$ by subtracting $m_{(i+1)}*\mathbf{G}$ from $\mathbf{U}_{(i+1)}$.)

The method according to said preferred second embodiment of this invention does not allow said $User_i$ to know the private key $x_{(i+1)}$ of said $User_{(i+1)}$, unlike the method according to said preferred first embodiment of this invention.

A preferred third embodiment of this invention concerns a certificate generation system wherein $User_{(i+1)}$ according to said preferred first or second embodiments of this invention certifies the association between the public key $\mathbf{Y}_{(i+2)}$ and the identification details $ID_{(i+2)}$ of a user termed $User_{(i+2)}$. Said public key $\mathbf{Y}_{(i+2)}$ can serve in any general public key cryptographic method, and it is not necessarily issued by said $User_{(i+1)}$ or effected by said certificate generation system.

Said $User_{(i+1)}$ generates a random $k_{(i+2)}$ and the certificate, which consists of the pair of values $\{\mathbf{T}_{(i+2)},s_{(i+2)}\}$, where $\mathbf{T}_{(i+2)} = k_{(i+2)}*\mathbf{G}$ and $s_{(i+2)} = H(ID_{(i+2)},\mathbf{Y}_{(i+2)},\mathbf{T}_{(i+2)})*k_{(i+2)} + x_{(i+1)}$.

A preferred fourth embodiment of this invention concerns a chained certificate verification system wherein a general user verifies the association between the public key $\mathbf{Y}_{(i+2)}$ and the identification details $ID_{(i+2)}$ of the user $User_{(i+2)}$ defined in the preferred third embodiment of this invention.

To effect said chained certificate verification, said general user is provided with said values $ID_{(i+1)}$ and $\mathbf{Y}_{(i+1)}$, the certificate, which consists of the pair of values

$\{s_{(i+2)},\mathbf{T}_{(i+2)}\}$, the public value $\mathbf{U}_0$ of the CA, and the reference information ID_j and $\mathbf{U}_j$, $j = 1, 2,\ldots, i+1$. Said general user then checks whether

$$s_{(i+2)}*\mathbf{G} = H(ID_{(i+2)},\mathbf{Y}_{(i+2)},\mathbf{T}_{(i+2)})*\mathbf{T}_{(i+2)} + H(ID_{(i+1)},\mathbf{U}_{(i+1)})*\mathbf{U}_{(i+1)} + H(ID_i,\mathbf{U}_i)*\mathbf{U}_i + H(ID_{(i-1)},\mathbf{U}_{(i-1)})*\mathbf{U}_{(i-1)} + \ldots + H(ID_1,\mathbf{U}_1)*\mathbf{U}_1 + \mathbf{U}_0.$$

A preferred fifth embodiment of this invention concerns a chained signature generation and verification system wherein $User_{(i+1)}$ according to said preferred first or second embodiments of this invention signs a message m. Said $User_{(i+1)}$ signs said message m by generating the signature which consists of the pair of values $\{\mathbf{T},s\}$, where $\mathbf{T} = k*\mathbf{G}$ for a random k, and $s = H(m,\mathbf{T})*k + x_{(i+1)}$.

A general user, provided with said signature $\{\mathbf{T},s\}$, effects a chained signature verification based on the public value $\mathbf{U}_0$ of the CA and the reference information ID_j and $\mathbf{U}_j$, $j = 1, 2,\ldots, i+1$. Said general user checks whether

$$s*\mathbf{G} = H(m,\mathbf{T})*\mathbf{T} + H(ID_{(i+1)},\mathbf{U}_{(i+1)})*\mathbf{U}_{(i+1)} + H(ID_i,\mathbf{U}_i)*\mathbf{U}_i + H(ID_{(i-1)},\mathbf{U}_{(i-1)})*\mathbf{U}_{(i-1)} + \ldots + H(ID_1,\mathbf{U}_1)*\mathbf{U}_1 + \mathbf{U}_0.$$

A preferred sixth embodiment of this invention concerns an alternative to any of said first to fifth preferred embodiments of this invention, in which the identification details of a user are not being used.

According to said preferred sixth embodiment of this invention, any notation of the form $H(ID_i,U_i)*\mathbf{U}_i$ or $H(ID_i,\mathbf{Y}_i,\mathbf{T}_i)$, used in any of said first to fifth preferred embodiments of this invention, is respectively replaced by $H(U_i)*\mathbf{U}_i$ or $H(\mathbf{Y}_i,\mathbf{T}_i)$.

All the above description of preferred embodiments has been provided for the purpose of illustration, and is not intended to limit the invention in any way. Many variations

can be made in the various methods and systems of the invention, without exceeding its scope.

CLAIMS

1. A method for effecting a chained key-issuing process over a finite group of points in which the discrete logarithm problem applies, wherein an issuing user ($User_i$), who possesses an issuing user public value ($\mathbf{U_i}$) and an issuing user private key (x_i), provides to a successor user ($User_{(i+1)}$) a successor user public value ($\mathbf{U_{(i+1)}}$) and a successor user private key ($x_{(i+1)}$), and where said issuing user, except for the Certifying Authority (CA), was himself a successor user in a preceding step in the chained key-issuing process, and where said Certifying Authority acts as the first issuing user in the chained key-issuing process, comprising the steps of:

(1) permitting said Certifying Authority to select a generating group-point ($\mathbf{G}$) whose exponentiations to various powers generate various group-points and a converting mathematical operation (H) which converts several input values into a scalar;

(2) permitting said Certifying Authority to posses a Certifying Authority private key (x_0);

(3) permitting said Certifying Authority to posses a Certifying Authority public value ($\mathbf{U_0}$), obtained by exponentiating said generating group-point to the power of said Certifying Authority private key ($\mathbf{U_0} = x_0 * \mathbf{G}$);

(4) permitting said issuing user ($User_i$) to possess said generating group-point ($\mathbf{G}$) and said converting mathematical operation (H) and the identification details ($ID_{(i+1)}$) of said successor user;

(5) permitting said issuing user ($User_i$) to possess an issuing user private key (x_i), where, except for the case in which said issuing user is said Certifying Authority, said issuing user private key was provided to said issuing user at a preceding stage in the chained key-issuing process (in which $User_i$ acted as a successor user in respect to an issuing $User_{(i-1)}$);

(6) permitting said issuing user ($User_i$) to calculate said successor user public value ($\mathbf{U_{(i+1)}}$) and said successor user private key ($x_{(i+1)}$) wherein:

- a successor user random value ($k_{(i+1)}$) is generated and said successor user public value ($\mathbf{U}_{(i+1)}$) is calculated by exponentiating said generating group-point to the power of said successor user random value ($\mathbf{U}_{(i+1)} = k_{(i+1)}*\mathbf{G}$);

- a successor user representing value ($H(ID_{(i+1)},\mathbf{U}_{(i+1)})$) is calculated by operating with said converting mathematical operation on said successor user identification details ($ID_{(i+1)}$) and said successor user public value ($\mathbf{U}_{(i+1)}$);

- said successor user private key ($x_{(i+1)}$) is calculated by multiplying said successor user representing value ($H(ID_{(i+1)},\mathbf{U}_{(i+1)})$) by said successor user random value ($k_{(i+1)}$) and adding said issuing user private key (x_i) to the product obtained by said multiplication ($x_{(i+1)} = H(ID_{(i+1)},\mathbf{U}_{(i+1)})*k_{(i+1)} + x_i$) and reducing the result modulo the order of said generating group-point;

(7) permitting said issuing user ($User_i$) to submit said successor user public value ($\mathbf{U}_{(i+1)}$) and said successor user private key ($x_{(i+1)}$) to said successor user ($User_{(i+1)}$).

2. A method for effecting a chained key-issuing process according to the method of Claim 1, where the issuing user ($User_i$) does not know the successor user private key ($x_{(i+1)}$), further comprising the steps of:

(i) permitting said successor user ($User_{(i+1)}$) to generate a first random value ($m_{(i+1)}$) and calculate a first intermediate group-point ($m_{(i+1)}*\mathbf{G}$) by exponentiating the generating group-point to the power of said first random value;

(ii) permitting said successor user to submit said first intermediate group-point ($m_{(i+1)}*\mathbf{G}$) to said issuing user ($User_i$);

(iii) permitting said issuing user to calculate a successor user public value ($\mathbf{U}_{(i+1)}$) and a successor user intermediate private key ($p_{(i+1)}$), wherein:

- a second random value ($k_{(i+1)}$) is generated and a second intermediate group-point ($k_{(i+1)}*\mathbf{G}$) is calculated by exponentiating said generating group-point to the power of said second random value;

- said successor user public value ($\mathbf{U}_{(i+1)}$) is calculated by adding said first intermediate group-point and said second intermediate group-point ($\mathbf{U}_{(i+1)} = m_{(i+1)}*\mathbf{G} + k_{(i+1)}*\mathbf{G}$);

- a successor user representing value ($H(ID_{(i+1)},\mathbf{U}_{(i+1)})$) is calculated in the way described;

- said successor user intermediate private key ($p_{(i+1)}$) is calculated by multiplying said successor user representing value ($H(ID_{(i+1)},\mathbf{U}_{(i+1)})$) by said second random value ($k_{(i+1)}$) and adding the issuing user private key (x_i) to the product obtained by said multiplication ($p_{(i+1)} = H(ID_{(i+1)},\mathbf{U}_{(i+1)})*k_{(i+1)} + x_i$) and reducing the result modulo the order of said generating group-point;

(iv) permitting said successor user to generate the successor user private key ($x_{(i+1)}$) by calculating said successor user representing value ($H(ID_{(i+1)},\mathbf{U}_{(i+1)})$) in the way described and multiplying said successor user representing value by said first random value ($m_{(i+1)}$) and adding said successor user intermediate private key ($p_{(i+1)}$) to the product obtained by said multiplication ($x_{(i+1)} = H(ID_{(i+1)},\mathbf{U}_{(i+1)})*m_{(i+1)} + p_{(i+1)}$) and reducing the result modulo the order of said generating group-point.

3. A certificate generation system for permitting a generating user who is a successor user ($User_{(i+1)}$) according to the method of Claim 1, to issue a certificate to a general user ($User_{(i+2)}$) where said certificate attests to the association between said general user public key ($\mathbf{Y}_{(i+2)}$) and said general user identification details ($ID_{(i+2)}$), where said general user public key was issued to said general user according to any known public key cryptographic method, the system comprising:

(1) means for permitting said generating user to generate a first random scalar ($k_{(i+2)}$);

(2) means for permitting said generating user to calculate a first part of a certificate ($\mathbf{T}_{(i+2)}$) by exponentiating the generating group-point to the power of said first random scalar ($\mathbf{T}_{(i+2)} = k_{(i+2)}*\mathbf{G}$);

(3) means for permitting said generating user to calculate a general user representing value ($H(ID_{(i+2)},\mathbf{Y}_{(i+2)},\mathbf{T}_{(i+2)})$) by operating with the converting mathematical operation on said general user identification details ($ID_{(i+2)}$) and said general user public key ($\mathbf{Y}_{(i+2)}$) and said first part of a certificate ($\mathbf{T}_{(i+2)}$);

(4) means for permitting said generating user to calculate a second part of a certificate ($s_{(i+2)}$) by multiplying said general user representing value by said first random scalar ($k_{(i+2)}$) and adding the private key ($x_{(i+1)}$) of said generating user to the product obtained by said multiplication ($s_{(i+2)} = H(ID_{(i+2)},\mathbf{Y}_{(i+2)},\mathbf{T}_{(i+2)})*k_{(i+2)} + x_{(i+1)}$) and reducing the result modulo the order of said generating group-point;

(5) means for permitting said generating user to submit said certificate to said general user, said certificate comprising of said first part of a certificate ($\mathbf{T}_{(i+2)}$) and said second part of a certificate ($s_{(i+2)}$).

4. A chained certificate verification system for permitting a verifying user to verify the authenticity of the certificate ($\mathbf{T}_{(i+2)}$ and $s_{(i+2)}$) issued to the general user ($User_{(i+2)}$) as defined in Claim 3, the system comprising:

(4) means for providing said verifying user with said certificate and with the general user public key ($\mathbf{Y}_{(i+2)}$) and with the general user identification details ($ID_{(i+2)}$) and with the Certifying Authority public value ($\mathbf{U_0}$) and with a plurality of pairs of values (ID_j and $\mathbf{U_j}$) consisting of the identification details and public values of all users ($User_j$, $j = 1, 2, \ldots, i+1$)) in the chained key-issuing process as defined in Claim 1, starting with the first successor

user $(User_1)$ after the Certifying Authority and ending with the generating user $(User_{(i+1)})$ as defined in Claim 3;

(2) means for permitting said verifying user to verify the validity of said certificate, wherein:

- a first scalar $(H(ID_{(i+2)},\mathbf{Y}_{(i+2)},\mathbf{T}_{(i+2)}))$ is calculated by operating with the converting mathematical operation on said general user identification details $(ID_{(i+2)})$ and said general user public key $(\mathbf{Y}_{(i+2)})$ and the first part of said certificate $(\mathbf{T}_{(i+2)})$;

- a first intermediate group-point $(H(ID_{(i+2)},\mathbf{Y}_{(i+2)},\mathbf{T}_{(i+2)})*\mathbf{T}_{(i+2)})$ is calculated by exponentiating said first part of the certificate $(\mathbf{T}_{(i+2)})$ to the power of said first scalar;

- users representing values $(H(ID_j,\mathbf{U}_j),\ j = 1, 2,\ldots, i+1)$ are calculated by operating with said converting mathematical operation on each pair of said plurality of pairs of values $(ID_j$ and $\mathbf{U}_j)$;

- users temporary group-points $(H(ID_j,\mathbf{U}_j)*\mathbf{U}_j,\ j = 1, 2,\ldots, i+1)$ are calculated for each user in said chained key-issuing process, starting with said first successor user $(User_1)$ and ending with said generating user $(User_{(i+1)})$, by exponentiating each said user public value $(\mathbf{U}_j)$ to the power of said user representing value $(H(ID_j,\mathbf{U}_j))$;

- a second intermediate group-point $(\mathbf{P})$ is calculated by adding all said users temporary group-points $(\mathbf{P} = H(ID_{(i+1)},\mathbf{U}_{(i+1)})*\mathbf{U}_{(i+1)} + H(ID_i,\mathbf{U}_i)*\mathbf{U}_i + H(ID_{(i-1)},\mathbf{U}_{(i-1)})*\mathbf{U}_{(i-1)} + \ldots + H(ID_1,\mathbf{U}_1)*\mathbf{U}_1)$;

- a third intermediate group-point $(\mathbf{Q})$ is calculated by adding said first intermediate group-point and said second intermediate group-point and the public value of said Certifying Authority $(\mathbf{Q} = H(ID_{(i+2)},\mathbf{Y}_{(i+2)},\mathbf{T}_{(i+2)})*\mathbf{T}_{(i+2)} + \mathbf{P} + \mathbf{U}_0)$;

- a fourth intermediate group-point ($s_{(i+2)}*\mathbf{G}$) is calculated by exponentiating the generating group-point to the power of the first part ($s_{(i+2)}$) of said certificate;

- the value of said fourth intermediate group-point ($s_{(i+2)}*\mathbf{G}$) is compared to that of said third intermediate group-point (**Q**) and the certificate is determined as being valid in the case of equality.

5. A chained signature generation and verification system for permitting a successor user ($User_{(i+1)}$) according to the method of Claim 1, to generate a signature and permitting a verifying party to verify said signature, the system comprising:

(1) means for permitting said successor user ($User_{(i+1)}$) to generate a signature on a message (m) wherein:

- a first scalar (k) is randomly generated;

- a first part of a signature (**T**) is generated by exponentiating the generating group-point to the power of said first scalar ($\mathbf{T} = k*\mathbf{G}$);

- a representing value ($H(m,\mathbf{T})$) is generated by operating with the converting mathematical operation on said message (m) and said first part of a signature (**T**);

- a second part of a signature (s) is calculated by multiplying said representing value ($H(m,\mathbf{T})$) by said first scalar (k) and adding the private key of said successor user ($x_{(i+1)}$) to the product obtained by said multiplication ($s = H(m,\mathbf{T})*k + x_{(i+1)}$) and reducing the result modulo the order of said generating group-point;

(5) means for permitting said successor user to submit said message (m) and said signature (**T** and s) to said verifying party, said signature comprising of said first part of a signature (**T**) and said second part of a signature (s);

(6) means for providing said verifying party with the Certifying Authority public value ($\mathbf{U}_0$) and with a plurality of pairs of values (ID_j and $\mathbf{U}_j$) consisting of the identification details and public values (ID_j and $\mathbf{U}_j$) of all users ($User_j$, $j = 1, 2, \ldots, i+1$)) in the chained key-issuing process as defined in Claim 1, starting with the first successor user ($User_1$) after the Certifying Authority and ending with said successor user ($User_{(i+1)}$);

(4) means for permitting said verifying party to verify the validity of said signature ($\mathbf{T}$ and s) on said message (m), wherein:

- said representing value ($H(m,\mathbf{T})$) is generated in the way described;

- a first intermediate group-point ($H(m,\mathbf{T})*\mathbf{T}$) is calculated by exponentiating said first part of the signature ($\mathbf{T}$) to the power of said representing value;

- users representing values ($H(ID_j,\mathbf{U}_j)$, $j = 1, 2, \ldots, i+1$) are calculated by operating with said converting mathematical operation on each pair of said plurality of pairs of values (ID_j and $\mathbf{U}_j$);

- users temporary group-points ($H(ID_j,\mathbf{U}_j)*\mathbf{U}_j$, $j = 1, 2, \ldots, i+1$) are calculated for each user in said chained key-issuing process, starting with said first successor user ($User_1$) and ending with said successor user ($User_{(i+1)}$), by exponentiating each said user public value ($\mathbf{U}_j$) to the power of said user representing value ($H(ID_j,\mathbf{U}_j)$);

- a second intermediate group-point ($\mathbf{P}$) is calculated by adding all said temporary group-points ($\mathbf{P} = H(ID_{(i+1)},\mathbf{U}_{(i+1)})*\mathbf{U}_{(i+1)} + H(ID_i,\mathbf{U}_i)*\mathbf{U}_i + H(ID_{(i-1)},\mathbf{U}_{(i-1)})*\mathbf{U}_{(i-1)} + \ldots + H(ID_1,\mathbf{U}_1)*\mathbf{U}_1$);

- a third intermediate group-point ($\mathbf{Q}$) is calculated by adding said first intermediate group-point and said second intermediate group-point and the public value of said Certifying Authority ($\mathbf{Q} = H(m,\mathbf{T})*\mathbf{T} + \mathbf{P} + \mathbf{U}_0$);

- a fourth intermediate group-point (s∗**G**) is calculated by exponentiating the generating group-point to the power of the first part (s) of said signature;

- the value of said fourth intermediate group-point (s∗**G**) is compared to that of said third intermediate group-point (**Q**) and the signature is determined as being valid in the case of equality.

6. A certificate generation system according to Claim 3, wherein the successor user ($User_{(i+1)}$) is defined according to Claim 2.

7. A chained certificate verification system according to Claim 4, wherein the chained key-issuing process is defined according to Claim 2.

8. A chained signature generation and verification system according to Claim 5, wherein the successor user ($User_{(i+1)}$) is defined according to Claim 2.

9. A method for effecting a chained key-issuing process, essentially as described and illustrated.

10. A certificate generation system, essentially as described and illustrated.

11. A chained certificate verification system, essentially as described and illustrated.

12. A chained signature generation and verification system, essentially as described and illustrated.

לוצאטו את לוצאטו
LUZZATTO & LUZZATTO
By ע״י

Ref:11002/00

שיטות ומערכות לאישור שרשרת יעיל

METHODS AND SYSTEMS FOR EFFICIENT CHAINED CERTIFICATION